In this table, we examined 16 drivers introduced in the previous session with 18 product features, and based on their influence, we have shown them with numbers 0, 1, 2, or 4. In this way, 0 means no relationship; one means low impact, two medium effects, and four high impacts.

As you can see in the total column, the lowest value is related to **P9:Dilever alarm notifications to the CSS SIEM (**Security information and event management) **system** and the highest value is 124, which is related to **P16:Substation resources must have secure access through a centrally supervised gateway.** 6 of the highest values were considered the most critical gaps, which my colleague will explain further.

As you can see in the total column each product feature has an specific value. 6 of the highest values were considered as the most critical gaps, which my colleague will explain further.

Despite its importance to modern society, the energy sector has adapted slower than other industries to digital technology due to its size and need for high system availability.

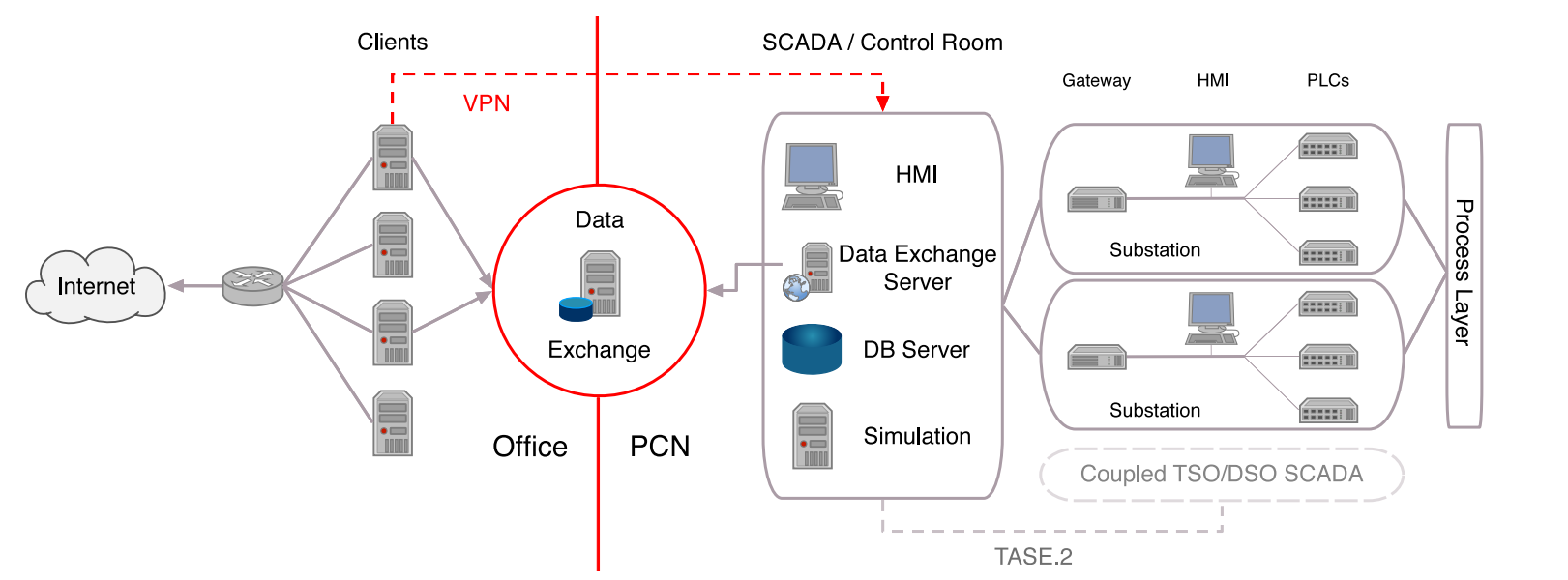
technology gets more widespread, and new technologies in the energy grid heavily rely on high-frequency monitoring cycles and adaptation to bottlenecks in the grid

The resulting increasing interconnection of power grids, which constitute critical infrastructure requiring special protection, raises severe security concerns

Yet, these systems are still used alongside modern technology and increasingly exposed to outside networks, such as the Internet. Likewise, the increasing use of digital and decentralized technology provides a larger attack surface. Resulting disruptions and wide-scale outages of electrical power have extensive social and economic consequences

cyber-attacks on power grids have already succeeded in causing temporary, large-scale blackouts in the recent past.

**2-Communication Infrastructure of Power Grids and Resulting Security Challenges**

We use the term grid exclusively to refer to the power grid and the term network for digital communication networks

(process control network (PCN) connects the control room of grid operation companies with their substations and field devices Resulting control messages are usually interpreted by a programmable logic controller (PLC) and then passed to the process layer. The control room typically contains a human-machine interface (HMI), a database (DB) server managing grid information, and a simulation server for pre-computing the effects of grid changes. Furthermore, the control room is connected to multiple substations (each containing at least a gateway, an HMI, and multiple PLCs) and can be coupled with other TSO/DSO SCADA systems for mutual control).

Data exchange between office network and PCN should only be handled through a dedicated data exchange server

Sometimes, though, as seen in the Ukraine attacks [21], there are other communication channels, such as VPNs, which allow direct communication between the office network and the PCN or remote maintenance lines for vendors or contractors.

**2-1-CIA Triad: Availability Is Key**

The triad of confidentiality, integrity, and availability (CIA) as the fundamental concept of information security has to be interpreted slightly differently in the energy sector

As availability is the most important measure in power grids, any measures ensuring the confidentiality and integrity of systems should never interfere with the availability of power delivery

**2-2-Balancing Generation and Consumption**

Electrical power grids rely on a stable grid frequency of either 50 Hz or 60 Hz due to the use of alternating current.

the operation reserve is separated in three different stages: primary operation reserve, secondary-reserve, and minute reserve.

(The primary control is a continuous frequency load control, where the controller is implemented as an droop control distributed to different power plants. The secondary-reserve and minute-reserve will be activated if the frequency derivation holds on. the secondary reserve has to be activated after 5 min of frequency derivation and will be replaced by the minute reserve after 15 min)

**2-3-Decentralization of Power Generation**

The rise of renewable energy has empowered many individuals and companies to enter the energy sector

Naturally, the security of their systems is not as tightly controlled as those of traditional energy companies.

**2-4- No Security in Process Control Networks**

Most devices used in power grids, such as protection devices or PLCs, are designed for multiple-decade use.

As grid operators often use their own separated networks over dedicated physical cables

Past attacks have shown that office networks (connected to the Internet) are allowing attackers to control devices crucial for grid operation

**2-5- Difficulty of Physical Network Changes**

Field devices in power grids have planned lifetimes which are measured not in years but decades

If possible, at all, modern security mechanisms have to be implemented in software only and run on the available hardware or be able to interface directly with the specialized devices used by grid operation companies, without affecting the availability of electricity supply

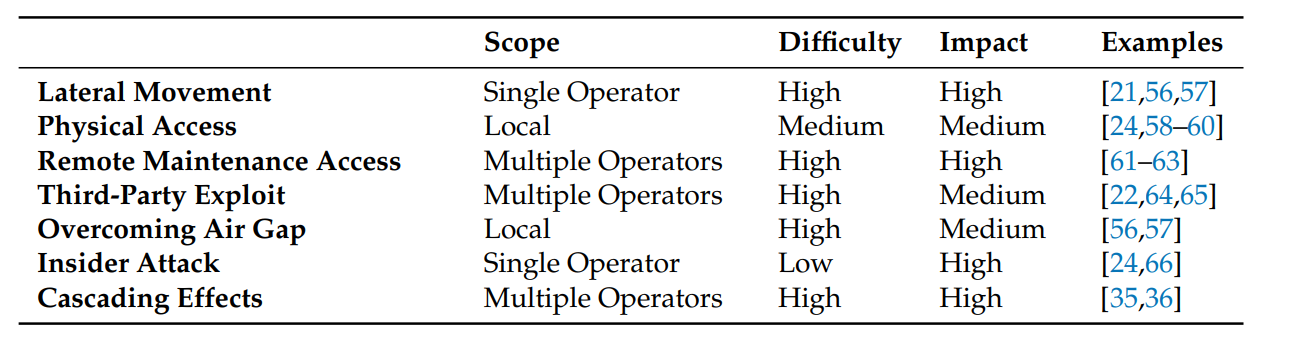
**2-6- Weakest Link Problem**

For attacks to have devastating consequences, an attacker does not have to target the largest grid operator

As long as the victim of an attack has control over enough power to affect the grid frequency, the attacker can leverage cascading effects to affect the whole power grid.

**3- Attack Vectors**

**3-1- Attack Vectors in Distribution and Transmission Grids**

Attackers can leverage different attack vectors to compromise the network of a transmission or distribution system operator with the goal of causing a blackout or at least considerable disturbance in the power grid.

**3-1- Lateral Movement from the Office Network**

In the attacks on Ukrainian grid operators in 2015, attackers gained access to the PCN through lateral movement from the office network

Allowing communications between PCN-connected devices and the office network might be necessary

Lateral movement from the office network is one of the most dangerous attack vectors for power system operators.

**3-2- Physical Access**

Energy providers often use their own dedicated cable networks for PCN communications. While this certainly provides an extra level of security, it does not offer any protection once an attacker has gained physical access to one device in the network.

**3-3- Remote Maintenance Access**

Manufacturers of control room software and hardware usually have a maintenance contract with the grid operators using their systems. To be able to debug these systems remotely or to deploy software updates, these systems are typically equipped with some form of remote maintenance access.

Depending on the technology used and security measures in place, attackers may try to exploit this maintenance access to gain access to the PCN

**3-4- Third-Party Exploit**

Attack vectors are not limited to the premises of grid operators. In fact, exploiting third-parties, such as suppliers or subcontractors, is one of the most dangerous and hard to control attack vectors.

If attackers are able to tamper with devices before they are installed at the grid operator, they might, e.g., install a covert channel for remote access.

**3-5- Overcoming Air Gap**

Even if PCNs are air-gapped, i.e., physically isolated from other networks, such as the office network to prevent lateral movement, attackers can still try to attack a PCN by strategically placing USB drives containing malware around a facility they are targeting.

**3-6- Insider Attack**

If an attacker already works within the energy sector or compromises an employee of a grid operator, the attacker might have direct access to the control room or field devices and could, therefore, directly control devices or introduce malware, even to air-gapped systems. Insider attacks are hard to predict and protect against.

**3-7- Cascading Effects**

Instead of having to compromise the network of one or more grid operators, an attacker may leverage cascading effects in the power grid to cause a power outage

**4-Attack Scenarios**

Different vectors can be used to attack distribution and transmission systems to disrupt vital control systems.

**4-1-Disconnecting Resources**

If an attacker has gained full access to the PCN, we can assume that the attacker is able to send arbitrary control commands to connected control systems.

In the attack on Ukraine in 2015, 225,000 consumers were disconnected from the grid, as attackers were able to control switches in multiple substations

**4-2- Injecting False Information**

If an attacker can only gain control over a small subset of field devices, he can still indirectly influence the power grid, e.g., by sending forged or manipulated sensor readings to the control room

**4-3- Denial of Service**

Even if attackers neither have full access to the PCN nor can inject (false) information, they may still be able to manipulate certain devices and effectively render them non-functional to launch a denial of service attack against parts of the power grid.

**Physical Access** & **Overcoming Air Gap**